

February 28, 2017

Via U.S. Mail:
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Via Electronic Mail:
Idtheft@oag.state.md.us

Re: GKIC
Notification of Potential Security Breach pursuant to Md. Code Ann. Comm. Law
§ 14-3504

To Whom it May Concern:

On behalf of our client, GKIC, a Chicago-based marketing services company (the “Company”), we hereby inform you of an incident arising from a spoof e-mail scam that affected the personal information of one (1) Maryland resident.

Description of the Incident. The incident occurred on February 21, 2017, when an e-mail that was designed to appear to be from a member of the Company’s senior management was sent to an employee in the Company’s payroll department instructing the employee to transmit all 2016 W-2 information for review. The employee who received the spoof e-mail was deceived by the e-mail, and mistakenly sent someone outside the Company the requested W-2 information. On February 24, the employee realized the mistake and raised the issue to senior management. The W-2 information that was mistakenly sent in response to the spoof e-mail included the affected Maryland resident’s name; Social Security number; 2016 wages; and all other information included in the 2016 W-2, excluding street address, city of residence, and ZIP Code.

Communication with Affected Maryland Resident. The affected Maryland resident was notified using the notification template enclosed with this letter as Exhibit A. The notification letter to the affected Maryland resident was hand delivered on February 28, 2017, and includes an offer for identity theft protection services at no cost to the affected individual. GKIC also sent a preliminary communication about the incident to affected individuals on February 24, 2017 in order to allow those individuals to take steps as soon as possible to protect themselves.

February 28, 2017

Page 2

Steps Taken Following the Incident. Immediately upon learning of the problem, the Company began reviewing all aspects of the incident, and taking steps to protect everyone involved. The Company has worked, and is working closely with outside legal counsel and other advisors, as well as law enforcement, to address the incident properly. The Company is reviewing its information governance practices and is implementing additional security measures designed to prevent a recurrence of such an incident in the future.

* * * * *

We trust that this letter and its enclosure provide you with the information required to assess this incident and the Company's response. Please let us know if you have any questions or if we may be of further assistance.

Sincerely,

Theodore P. Augustinos

Theodore P. Augustinos

w/ permission

Enclosure

CyH

EXHIBIT A



February 28, 2017

To: All GKIC Team Members

On February 24, 2017, we provided you with preliminary notice of an unfortunate incident that involved your personal information. This letter provides additional information, guidance, and an offer of services at no cost to you, to help you protect yourself.

What Happened? As we informed you previously, on February 21, 2017, an email that was designed to appear to be from a member of our senior management was sent to an employee of our payroll department. The "spoof" email instructed the employee to transmit all 2016 W-2 information for review. The employee who received the spoof email was deceived by the email, and mistakenly sent someone outside our company your W-2 information. On February 23, the employee realized the mistake and raised the issue to senior management.

What Information Was Involved? Your W-2 information that was mistakenly sent in response to the spoof email included the following:

- Name
- Social Security number
- 2016 Wages and
- All other information included in your 2016 W-2, excluding your street address, city of residence and zip code

What Are We Doing? GKIC has reviewed all aspects of this incident, and has taken steps to protect everyone involved. We are working closely with outside legal counsel and other advisors, as well as law enforcement, to address this incident properly. We have engaged **LifeLock®** to provide services that are being offered at no cost to you to assist you in protecting yourself against possible risks resulting from this incident. Enclosed is enrollment information for these services, as well as additional guidance on how to protect yourself. We are also implementing additional security measures internally designed to prevent a recurrence of such a breach of sensitive data and to protect the privacy of all of GKIC's valued employees and their information.

What Can You Do? First, you can follow the enclosed instructions to activate your one-year subscription for the identity theft protection services provided by **LifeLock®**, which we are offering at no cost to you. Enrollment for these services closes on April 30, 2017; you must enroll by that date in order to take advantage of this offering.

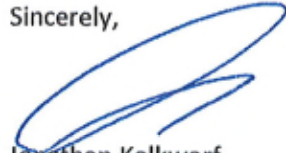
As always, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, please visit www.annual-creditreport.com or call (toll free) 877/322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report. Also enclosed is additional guidance, as well as certain information applicable to residents of particular states.

You may also want to take measures designed to protect yourself from tax-related identity theft, such as by:

- Reviewing the recommended actions by the Internal Revenue Service at www.irs.gov/identitytheft.
- Filing a Form 14039, Identity Theft Affidavit, if your own tax return rejects because of a duplicate Social Security number or if instructed to do so by the IRS.

For More Information. Again, we regret that this incident occurred, and apologize for any concern or inconvenience it may cause. We will contact you again soon with enrollment instructions for your free services, and additional guidance to help you protect yourself. Please call us at [toll free number] with any questions or concerns, and please contact LifeLock using the enclosed instruction letter to enroll in the services we are offering at no cost to you.

Sincerely,

A handwritten signature in blue ink, appearing to read 'Jonathan Kalkwarf', is written over the printed name.

Jonathan Kalkwarf
Director of Finance

Enclosures

Information Concerning Identity Protection Services

GKIC has retained LifeLock® to provide one (1) year of complimentary identity theft protection.

To get protection immediately at no cost to you:

1. Call **1-800-899-0180** or visit **www.lifelock.com** to enroll.
 - Click on "START MEMBERSHIP"
 - On the bottom of the next page enter Partner/Promo code **GKIC2017**
2. Then enter your Member ID.
 - Your Member ID is your first name last name plus your 5-digit zip code.
 - Ex. JOHNNORTON12345

LifeLock's specialized team of telephone representatives is available 24 hours a day, seven days a week to help you enroll in LifeLock.

You will have until April 30, 2017 to enroll in this service.

Once you have completed the LifeLock enrollment process, the services will be in effect immediately. Your LifeLock Ultimate Plus™ membership includes:

- ✓ LifeLock Identity Alert® System†
- ✓ Fictitious Identity Monitoring
- ✓ Investment Account Activity Alerts†
- ✓ Checking and Savings Account Application Activity Alerts†
- ✓ Bank Account Takeover Alerts†
- ✓ Online Annual Tri-Bureau Credit Reports & Scores
- ✓ LifeLock Privacy Monitor
- ✓ Live, U.S.-based Member Service Support
- ✓ Identity Restoration Support
- ✓ Priority Live Member Service Support

LifeLock backs up its services with its \$1 Million Service Guarantee‡.

No one can prevent all identity theft.

† LifeLock does not monitor all transactions at all businesses.

‡ Stolen Funds Reimbursement benefits and Service Guarantee benefits for State of New York members are provided under a Master Insurance Policy underwritten by State National Insurance Company. Benefits for all other members are provided under a Master Insurance Policy underwritten by United Specialty Insurance Company. Under the Stolen Funds Reimbursement, LifeLock will reimburse stolen funds up to \$25,000 for Standard membership, up to \$100,000 for Advantage membership and up to \$1 million for Ultimate Plus membership. Under the Service Guarantee LifeLock will spend up to \$1 million to hire experts to help your recovery. Please see the policy for terms, conditions and exclusions at LifeLock.com/legal.

ADDITIONAL GUIDANCE AND DISCLOSURES:

Your taking steps to protect yourself may include contacting credit reporting agencies as further described below. The following is contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Order your Free Credit Report. We recommend that you remain vigilant for incidents of fraud and identity theft by reviewing your account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

You can order your annual free credit report at www.annualcreditreport.com or by calling toll free 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form, which you can obtain from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov), to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Note that thieves may hold stolen information to use at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

Notice for residents of Georgia and Maryland: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain these additional report(s).

Fraud Alert. We recommend that you place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for 90 days. You can renew it after 90 days. Note that a fraud alert in your file can protect you, but also may delay you when you seek to obtain credit.

Security Freeze. You also may want to consider contacting the major credit bureaus at the telephone numbers, websites, or addresses above to add a security freeze to your credit file. A security freeze means potential creditors cannot get your credit report. That makes it less likely that an identify thief can open new accounts in your name. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. When adding a security freeze to your credit file, you must provide the following information (and the same information for your spouse if you are also requesting a security freeze for your spouse as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles.

Your request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. (You must review your state's requirement(s) and/or credit bureau requirement(s) for the specific document(s) to be submitted.) The credit reporting agencies may charge a fee to place a freeze, temporarily lift it or permanently remove it. The fee is waived if you are a victim of identity theft and have submitted a valid investigative or law enforcement report or complaint relating to the identity theft incident to the credit reporting agencies. The cost to place and lift a freeze depends on state law. Find your state Attorney General's office at naag.org to learn more.

You may obtain additional information about fraud alerts and security freezes from the Federal Trade Commission, or the consumer reporting agencies. Contact information is provided below for the FTC and above for the consumer reporting agencies.

Contact the Federal Trade Commission and the Office of your State Attorney General. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you

should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

Notice for Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

Reporting of identity theft and obtaining a police report.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, file a police report. Get a copy of the police report; you may need it to clear up the fraudulent debts.

If your personal information has been misused, visit the FTC's site at IdentityTheft.gov to get recovery steps and to file an identity theft complaint. Your complaint will be added to the FTC's Consumer Sentinel Network, where it will be accessible to law enforcers for their investigations.